



**DIVISION OF CHILD SUPPORT ENFORCEMENT
COMPUTER RISK MANAGEMENT PROGRAM**

**From The Office Of State Auditor
Claire McCaskill**

Department officials need to develop a risk management program, improve disaster recovery planning, and improve controls over access to sensitive division information.

**Report No. 2003-44
May 20, 2003
www.auditor.state.mo.us**

PERFORMANCE AUDIT



Office of
Missouri State Auditor
Claire McCaskill

May 2003

Disbursing child support checks could be interrupted in a disaster due to inadequate data recovery plans, unauthorized access to system also possible

This audit assessed how well the state can recover data after unexpected interruptions to the state's child support computer system, which disburses child support checks. Division of Child Support Enforcement (DCSE) distributed about \$447 million in child support checks to parents during fiscal year 2002. The computer system also maintains confidential child support data, such as parental and court-ordered information, and is not adequately protected from unauthorized access.

Disaster recovery planning efforts have been inadequate

DCSE has not updated or used its disaster recovery plan since 1994, when the contractor developed the plan. Instead, DCSE personnel have relied on the Department of Social Services' disaster recovery plan. However, the department's plan referred to DCSE's outdated 1994 plan and did not specifically address procedures to recover DCSE's computer system. In addition, the department has a reactive recovery plan, in which data recovery teams meet after a disaster occurs and decide what is needed. (See page 6)

Backup and recovery procedures were inadequate

Federal information system control guidelines state an entity should have the ability to restore data files if lost in a disaster. However, auditors found backup files were not properly rotated to an off-site location to avoid disruption if data is lost or damaged. In addition, no inventory existed for the off-site storage facility ensuring availability of proper data and documentation. (See page 7)

DCSE's computer system was not reestablished in some disaster recovery tests

The department could not reestablish DCSE's computer system in 2001 and 2002 disaster recovery tests. While personnel recovered DCSE's system in the 2003 test, they did not have enough time to complete all test procedures. Plan deficiencies exposed in the first two tests included incomplete back up data to recover the system. (See page 9)

Confidential, sensitive child support information not always protected

The department has risked having current and former employees gain unauthorized access to DCSE's computer system. Improvements are needed in controlling access to the computer system relating to: revoking terminated employees' passwords, keeping multiple user IDs to a minimum, sharing user IDs, checking criminal background of all employees,

YELLOW SHEET

and restricting system access to users from remote locations. (See page 13)

Unrestricted access to sensitive data has resulted in some abuses

In the past 4 years, DCSE officials reprimanded or suspended 12 employees who allegedly misused sensitive computer information. For example, a DCSE technician, who rented an apartment to a custodial parent, electronically checked if the parent received a child support payment when she had not paid rent owed to the technician. When the technician saw the parent received the check, the technician asked for the rent. In addition, technicians have access to all cases, not just the cases in their respective caseloads. Such unlimited access has led to some of the abuses noted. (See page 17)

All reports are available on our website: www.auditor.state.mo.us

**DIVISION OF CHILD SUPPORT ENFORCEMENT
COMPUTER RISK MANAGEMENT PROGRAM**

TABLE OF CONTENTS

	<u>Page</u>
STATE AUDITOR’S REPORT	1
INTRODUCTION.....	3
RESULTS AND RECOMMENDATIONS.....	5
1. Officials Have Not Ensured Essential Operations Will Continue if Computer Support is Lost	5
Conclusions.....	11
Recommendations.....	12
2. Adequate Controls Have Not Been Established to Safeguard Access to Sensitive Information	13
Conclusions.....	21
Recommendations.....	22
 APPENDIXES	
I. SAMPLE METHODOLOGY AND RESULTS.....	23
II. COMMENTS FROM THE DEPARTMENT OF SOCIAL SERVICES	25

ABBREVIATIONS

DCSE	Division of Child Support Enforcement
ID	Identification
FISCAM	Federal Information System Controls Audit Manual
CFR	Code of Federal Regulations



CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden, Governor
and
Steve Roling, Director
Department of Social Services
Jefferson City, MO 65102

Over half a million Missouri children and their custodial parents rely on the state to collect and disburse child support payments, which are tracked and managed through the Division of Child Support Enforcement's (DCSE) computerized system. Because of the computerized system's critical role, we focused review efforts on the management and oversight of DCSE's computer security program. Specific objectives included determining whether DCSE and/or the Department of Social Services (department) officials have (1) established an adequate risk management program, and ensured essential services can be continued in case of a disaster, or other unexpected interruptions; and (2) protected DCSE's computerized system and sensitive data against unauthorized access.

Improvements are needed in the management and oversight of DCSE's computer security program. DCSE officials have not established a risk management program, or developed an adequate disaster recovery plan. Policies and procedures establishing a risk management program, and performing risk assessments have not been developed. Officials also have not updated, or used, DCSE's disaster recovery plan developed by DCSE's contractor in 1994. Instead, they have relied on the department for disaster recovery planning efforts. However, the department's planning efforts have not adequately addressed (1) critical resources and data needed, (2) backing up and recovering data, (3) the identification of facilities used to store critical resources and data.

Improvements are also needed in controlling access to DCSE's computerized system and sensitive information. Improvements are needed in (1) revoking employee user identification (ID) codes and resetting user passwords; (2) limiting the sharing and issuing of multiple user IDs, (3) performing background checks on users; (4) reviewing access rights of users, and controlling access to security software; and (5) restricting access to the computerized system by users from remote locations.

We have included recommendations to improve the management and oversight of DCSE's computer security program.

We conducted our work in accordance with applicable standards contained in *Government Auditing Standards* issued by the Comptroller General of the United States and included such tests of the procedures and records as were considered appropriate under the circumstances. We obtained oral comments from department officials in a meeting on March 31, 2003, and written comments from the Director of the Department of Social Services dated April 29, 2003. We conducted our work between July 2002 and January 2003.

A handwritten signature in black ink, reading "Claire McCaskill". The signature is fluid and cursive, with the first name "Claire" and last name "McCaskill" clearly distinguishable.

Claire C. McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	Kirk R. Boyer
Audit Manager:	Robert D. Spence, CGFM
Auditor In-Charge:	Susan Beeler
Audit Staff:	Andrea Paul
	Dana Gerke

INTRODUCTION

The Family Support Act of 1988¹ required each state to develop an automated child support tracking system. Beginning in 1993, the Division of Child Support Enforcement (DCSE) worked with the Department of Social Services' (department) Information Services and Technology (technical support) Division and an independent contractor to develop a computer system fulfilling this act. DCSE implemented the Missouri Automated Child Support System (computerized system) in September 1998 and the contractor maintained the system until September 2001, when the department's technical support division assumed this responsibility. DCSE owns the data residing on the computerized system and the system is located on the Office of Administration's State Data Center (data center) mainframe. The department is considered a customer of the data center and informs the data center of what it needs (such as what data to backup). The data center then performs the related services. Technical support division guidance defines the purpose of the computerized system as assisting in the collection and disbursement of child support through enforcement of existing judicial and administrative orders; location of custodial and non-custodial parents; establishment of paternity and orders of support; and other activities.

During fiscal year 2002, DCSE's computerized system processed approximately \$447 million in child support collections. A contractor hired by DCSE collects child support and sends electronic receipt files to the computerized system. The system creates disbursement files, which the contractor picks up electronically and sends to a bank for payment. In addition to collection and disbursement information, confidential child support data such as the identity of custodial and non-custodial parents, and court ordered information, is maintained on the system. Federal regulations² require disbursement of child support payments within two business days of receipt, and the loss of DCSE's computerized system would delay the distribution of child support payments.

Several other entities rely on the computerized system including the department's Division of Medical Services and Division of Family Services, the Department of Health and Senior Services, circuit court clerks, prosecuting attorney offices, and state contract employees. Individuals having access to information on the system are required to have a user identification (ID) code. As of July 11, 2002, there were 7,825 active user IDs on the system.

Recognized organizations have established computer security guidelines

According to the National Institute of Standards and Technology, the U.S. Critical Infrastructure Assurance Office, and the U. S. General Accounting Office, effective computer security controls and processes are essential to protect against unauthorized acts. These nationally and internationally recognized organizations have issued computer security guidelines noting aspects of an effective computer security program including (1) periodic risk and vulnerability assessments, (2) disaster recovery or continuity of operation plans, (3) effective access controls, and (4) periodic evaluations of in-place controls to ensure they are effective.

¹Public Law 100-485.

²Federal regulation 42 USC 654b provides for the loss of federal funds if two-day payment criterion is not met.

Methodology

Our review focused on determining factors adversely affecting DCSE's ability to protect its computer system and data against unauthorized access, and recovery of computer processing operations in case of a disaster or other unexpected interruptions. Because the state does not have published computer security standards, policies, or guidelines for state agencies to follow, we based our work on the U. S. General Accounting Office's Federal Information System Controls Audit Manual (FISCAM). This manual provides guidance for reviewing information system controls affecting integrity, confidentiality, and availability of computerized data. In addition to the manual, we used generally accepted computer security program principles and guidelines published by the National Institute of Standards and Technology, and the U.S. Critical Infrastructure Assurance Office.

To accomplish our objectives, we reviewed the department's and DCSE's policies and procedures, and records related to computer security. In addition, we interviewed knowledgeable department and DCSE personnel, and observed and field tested controls to determine if system controls were in place. We observed the last two disaster recovery tests, which occurred in 2002 and 2003, and analyzed documented results of a 2001 disaster recovery test.

We tested statistical samples of user IDs³ to determine the number of user IDs revoked due to a monthly inactivity report and the number of newly hired or newly transferred department employees with computerized system access who had not had background checks. Because the objective of our review was to assess the overall effectiveness of DCSE's computer general controls, we did not evaluate application controls.

³See Appendix I, page 23, for information on sample results.

RESULTS AND RECOMMENDATIONS

1. Officials Have Not Ensured Essential Operations Will Continue if Computer Support is Lost

The department has not ensured essential services can be continued in the event of a disaster, or other occurrences, resulting in the loss of computer support. This situation has occurred because DCSE has not established a risk management program and its disaster recovery planning has not been adequate. DCSE has not performed risk assessments needed to help formulate security policies and procedures, and it has depended on the department's technical support division for disaster recovery planning, which has been inadequate. Until officials address these issues, DCSE will be at risk of not meeting its primary mission—assuring child support payments are provided to custodial parents and dependant children in a timely manner.

DCSE has not established a risk management program

DCSE has not established formal policies and procedures establishing a risk management program. A risk management program should include risk assessments, which are used to help formulate and modify security policies and procedures, according to the FISCAM. The FISCAM also states risk assessments should consider both sensitivity and integrity of data, and the risks to data inherent in an entity's systems. These risks include those posed by authorized internal and external users, as well as unauthorized outsiders who may try to gain access to the systems. Risk assessments help ensure all vulnerabilities and threats to the computerized system and data are identified. Decisions can then be made regarding which risks to accept and which to mitigate through security controls such as disaster recovery planning and controlling access to sensitive data. In addition, the FISCAM states risk assessments are considered beneficial when they include independent personnel.

According to a DCSE official, DCSE has not established such a program because it relies on the department's technical support division, which maintains DCSE's computerized system, to assess risk on the system and data.

Department lacks policies and procedures on risk assessments

The department's technical support division has not established guidance on conducting risk assessments for department systems—which includes DCSE's computerized system. This guidance includes policies and procedures for assessing risk and the frequency of the assessments. According to the technical support division's computer security official,⁴ the department has had a security manual since at least 1992. However, the security manual does not address risk assessments. According to the security official, the department has not established policies and procedures for conducting risk assessments because “we are still trying to get our feet under us.” He also stated no risk assessments had been conducted since 1996 because the department had not had the “time or manpower,” and also cited the recent “budget crunch.”

⁴This is the Department of Social Services and Department of Health and Senior Services Security Manager.

Risk assessment performed in 1996 disclosed weaknesses

DCSE's contractor responsible for developing and implementing its computerized system published a risk assessment in May 1996, prior to the system's full deployment. The risk assessment focused on DCSE, prosecuting attorney, and circuit clerk offices and highlighted several vulnerabilities. The top five include fire, privacy, policy, training, and accountability. The identified safeguards, if implemented by DCSE, would substantially reduce or possibly eliminate losses if identified threats occurred. The safeguards include:

- establishing a visitor control system,
- developing an organizational structure,
- developing a system of audit trails,
- conducting risk analyses,
- developing a security plan,
- establishing a program for property inventory control,
- developing an access control system, and
- implementing a coordinated detection system.

The risk assessment report also identified immediate steps needed to improve the overall security and safety of DCSE. These steps included developing visitor sign-in procedures; marking documents as classified, private, or personal; developing a contingency plan for the entire computerized system; standardizing fire, water, and smoke detectors; establishing a complete set of emergency procedures; maintaining adequate fire suppression equipment on site; documenting and reviewing a policy manual, training curriculum, and operating procedures; ensuring passwords are not shared; and training staff on policies and procedures.

According to a DCSE official, some of the report recommendations have been implemented; however, no formal follow-up of the recommendations has occurred. As a result, the official could not provide documentation supporting implementation of any safeguards or recommendations.

Disaster recovery planning efforts have not been adequate

The contractor who developed DCSE's computerized system prepared DCSE's disaster recovery plan in 1994. However, since 1994, personnel have not updated the plan or used it for testing purposes. According to the FISCAM, a comprehensive disaster recovery plan should reflect current conditions, clearly assign responsibilities for recovery, and include detailed instructions for restoring operations. We found DCSE's 1994 plan had not been updated to address (1) subsequent changes to the computerized system, (2) the need to reestablish communication lines with DCSE's contractor responsible for issuing child support checks, (3) reestablishing DCSE's

computerized system capability on a statewide basis,⁵ and (4) identifying the responsibilities of those carrying out the disaster recovery plan.

In lieu of updating and using its own disaster recovery plan, DCSE has relied on the department's disaster recovery plan developed by technical support division personnel. However, the department's disaster recovery plan does not address recovery procedures related to DCSE's computerized system. Instead, the plan refers to the 1994 disaster recovery plan prepared by the contractor who developed DCSE's computerized system. According to the department's disaster recovery plan, the contractor responsible for developing the computerized system also had responsibility for creating a disaster recovery plan and adequate backup capabilities for the system. The plan also stated the department would work with the contractor to periodically review and update the 1994 disaster recovery plan and assume disaster recovery planning efforts once the contract expired, which occurred in September 2001. However, the 1994 disaster recovery plan has not been reviewed and updated, though it should be done, according to the security official.

DCSE relies on department for planning efforts

Our review of the department's disaster recovery plan, prepared by technical support division personnel, also disclosed deficiencies. For example, the plan does not document specific disaster recovery procedures for recovery of department systems. Instead, it establishes disaster recovery teams that will meet once a disaster occurs to develop disaster recovery action plans. Furthermore, the department's plan does not identify (1) resources and data necessary in the event of a disaster, (2) backup and recovery capabilities needed for successful disaster recovery, and (3) facilities used to house sensitive and critical equipment and data. In addition, recent disaster recovery efforts highlighted problems with disaster recovery testing.

Disaster recovery plan does not identify critical resources and data

The department does not have formal procedures requiring a listing of critical operations and data, or of resources needed to support critical operations. Instead, the technical support division maintains a prioritization listing of all department systems. In addition, in commenting on a draft of this report, the technical support division provided us a listing of resources the data center will allocate to the department to assist in disaster recovery. However, these listings are not complete. For example, technical support division personnel did not identify critical resources such as all hardware, software, communications lines and system documentation, needed to maintain computerized operations and to successfully recover and use the application. According to the FISCAM, it is essential for management to identify critical operations and data and the resources needed to recover and support them.

Backup and recovery procedures are not adequate

The department has not established adequate backup and recovery procedures to restore DCSE's computerized system in the event of a disaster. FISCAM states an entity should

⁵There are 22 field offices, as well as circuit clerk and prosecuting attorney offices using the computerized system on a frequent basis.

maintain an ability to restore data files, which may be impossible to recreate if lost. We found two major problems with backup procedures.

- Backup files are not properly rotated off-site to avoid disruption if data is lost or damaged. The July 2002 disaster recovery test summary stated technical support division personnel found the data center did not have a backup copy of the catalog, which is the master index of the data files, in the off-site storage vault. Therefore, the catalog was not available to be sent to the out-of-state recovery site. Instead, the department had to send an on-site tape, containing the catalog, to the out-of-state recovery site to continue the recovery exercise. In a real disaster, the on-site tape could have been destroyed.
- There are no policies or procedures related to off-site storage of system and application documentation. As a result, program libraries were not backed up and sent to the backup vault prior to the disaster recovery test in July 2002, and still had not been done, as of December 31, 2002. Without the proper program libraries, technical support division personnel could not successfully use the recovered database.

In addition, inventories are not performed at the off-site storage facility to ensure the proper data and documentation is available in a disaster or other disruption in business processes. The department's disaster recovery plan states backups should be checked for accuracy at least semi-annually. However, according to technical support division personnel, no one has inventoried the off-site vault.

Facilities used to house critical resources have not been identified

Technical support division personnel do not maintain a list of facilities housing critical resources, and current policies do not require such identification. According to the FISCAM, entities should identify facilities housing sensitive and critical resources to evaluate the effectiveness of security controls.

When we requested technical support division personnel identify sensitive or critical resources and where they are housed, they provided a list. However, this list did not include information on one of the warehouses where system backups are stored and all physical resources, such as terminals.

In commenting on a draft of the report, a technical support division official acknowledged the department's disaster recovery plan had not been updated or adequately documented. Furthermore, the official stated disaster recovery planning has been adequate based on results of disaster recovery testing and a revised plan dated April 9, 2003. However, the FISCAM states a disaster contingency plan should be documented, and should be detailed enough so that its success does not depend on the knowledge or expertise of individuals. The revised plan does not meet these accepted standards because it does not specifically address DCSE's computerized system and we identified problems associated with disaster recovery testing.

Department testing highlighted disaster recovery problems

During the department's disaster recovery tests in 2001 and 2002, technical support division personnel were not successful in reestablishing DCSE's computerized system to an operable state. In the 2003 test, while personnel recovered the system, they did not accomplish all testing goals. The test assumed the main data center site was inoperable. Therefore, all tapes needed for recovery housed in the off-site backup vault were sent to the out-of-state recovery site to initiate the recovery testing. The data center initiated disaster recovery testing and had responsibility for reestablishing the mainframe during the testing. After reestablishing the mainframe, the departments participating in the test were responsible for recovering their own systems. The Department of Social Services chose to participate in the three tests we reviewed. The January 2001 disaster recovery testing disclosed the following problems.

- The department's technical support division personnel did not successfully recover the computerized system database because image copies were not vaulted and physical backups did not include all volumes used for production.
- DCSE did not include applications testing to ensure the system functioned properly, if a successful recovery had occurred.

After the January 2001 testing, the department's technical support division personnel did not verify disaster recovery test action items had been corrected for deficiencies identified during the test. We found 5 of 23 action items, resulting from the January 2001 test, were not completed prior to the July 2002 test. For example, one action item recommended providing improved documentation outlining backups created and recovery processes to be followed. The security official stated several actions have been taken but could not provide documentation showing any changes had been made from January 2001 to July 2002.

In addition, the security official provided documentation confirming implementation of many action items during the July 2002 exercise, but not prior to the test.

The technical support division's July 2002 disaster recovery testing summary disclosed the following deficiencies.

- Department technical support division personnel could only recover DCSE's computerized system database by sending an on-site backup tape to the disaster recovery contractor located in another state. In a real disaster, this tape would not have been available because it was not in the off-site vault, according to the security official. Even with the backup tape, DCSE personnel could not use the database because of the missing program code, and as a result, applications teams could not test the database. Therefore, department technical support personnel could not successfully recover DCSE's database to a usable state.

Technical support division personnel said if they had more time, they could have re-created the program code. However, because of the time limit set on the disaster

recovery exercise, they cannot be certain they could re-create this program code in a real disaster situation.

- The testing also did not include re-creating the communications link between DCSE's contractor that distributes payments to custodial parents and DCSE's computerized system database. The link, a communications router connecting DCSE's system to the contractor, which enables file transfers to the contractor to take place, is a critical component enabling the contractor to distribute child support payments to custodial parents and children.

According to the director of the department's technical support division, a manual tape exchange could be used in lieu of the link. However, the contract with the current contractor was signed prior to the technical support division taking over the system. Therefore, the manual tape exchange has not been tested by the department's technical support division. Additionally, this proposed method of providing DCSE's contractor with a physical tape is not addressed in department or DCSE disaster recovery plans.

- No applications testing took place on DCSE's computerized system because department technical support division personnel could not recover DCSE's system to a usable state. In addition, the applications testing process planned by DCSE personnel did not include testing the day-to-day users' access to the system due to the cost and time constraints of bringing field staff into the Jefferson City office, according to a DCSE official. Instead, DCSE managers planned to conduct some limited testing in this area. A DCSE official indicated that DCSE managers conducting the testing serve as business liaisons between the technical support division and the day-to-day users of the system. Therefore, the DCSE managers are aware of the needs of the day-to-day users. However, it is a good business practice to have day-to-day users test the system to ensure all needed data and screens are available. If such tests are not possible, the day-to-day users should, at a minimum, review the test documents.
- The test, as well as the disaster recovery plan, did not address bringing the system up on a statewide basis even though 22 field offices, as well as circuit court clerks and prosecuting attorney locations also use DCSE's system daily. According to the security official, if the department's technical support personnel attempted to bring up the system statewide, the communications line carrying information to and from the recovery site would not be sufficient to carry all users of the system. Therefore, in a disaster, if department technical support personnel recovered the system, all statewide users could not use the system.

The department's latest disaster recovery testing occurred in March 2003. The 72-hour test assumed a disaster occurred on February 5, 2003. Technical support division personnel were to recover department systems, which included DCSE's computerized system, through February 4, 2003. According to the security official, the following difficulties were experienced while recovering DCSE's computerized system.

2003 testing
could not be
completed

- Department personnel could only recover DCSE's computerized system through February 3, 2003, one day short of the test goal, because technical support division personnel found state data center personnel failed to vault the most recent database logs. The same problem occurred during the January 2001 test, and may have occurred during the July 2002 test, according to the security official. Approximately 71.5 hours into the testing, the technical support division recovered DCSE's system.
- Once DCSE's system had been recovered, a DCSE official had 30 minutes to perform applications testing. However, 7 of the 25 scheduled test items could not be performed because of time constraints and because personnel conducting the test did not have the proper security clearance.

Conclusions

DCSE officials have not developed a risk management program, and lack policies and procedures on conducting risk assessments. A risk management program is needed to help officials formulate and/or modify security guidance and identify security risks to DCSE's computerized system. The division's contractor performed a risk assessment in 1996, as part of its efforts to develop DCSE's system; however, division officials have no documented evidence of corrective action and have not performed any additional risk assessments.

DCSE's disaster recovery plan, developed by its contractor in 1994, has not been updated or used by DCSE. Instead, division officials rely on the department for disaster recovery planning and testing. However, the department's disaster recovery plan does not address recovery procedures related to DCSE's computerized system and instead, refers to the division's outdated 1994 plan. In addition, the department's disaster recovery plan does not address resources and data necessary in the event of a disaster, backup and recovery capabilities needed for successful disaster recovery, and facilities used to house critical resources. System and application documentation are not stored at the off-site location and inventories are not performed at this location.

Disaster recovery testing in 2001 and 2002 highlighted problems and disclosed the inability of technical support division personnel to successfully reestablish DCSE's computerized system to an operable condition. In addition, testing did not include planned applications testing by day-to-day users of the system. Not all deficiencies noted during disaster recovery testing in 2001 had been implemented and tested prior to the 2002 disaster recovery test. Although technical support division personnel recovered DCSE's system in the March 2003 disaster recovery test, some problems were experienced. The inability of technical support division personnel to successfully conduct disaster recovery testing in 2001 and 2002, along with problems experienced in the 2003 test, illustrates the need for adequate planning efforts. DCSE and department officials need to work together to develop an effective risk management program and an adequate disaster recovery plan to assure DCSE's computerized system is protected, can be recovered in a disaster, and initiates timely child support payments.

Recommendations

We recommend the Director of the Department of Social Services:

- 1.1 Develop a comprehensive risk management program, which would include policies and procedures requiring:
 - Risk assessments, specifying their frequency, and the responsible personnel.
 - Risk assessments when major system changes occur.
- 1.2 Develop a comprehensive and current disaster recovery plan for DCSE's computerized system which:
 - Reestablishes communication lines with the DCSE contractor who issues child support checks, reestablishes DCSE's computerized system capability on a statewide basis, and identifies the responsibilities of those carrying out the disaster recovery plan.
 - Identifies and prioritizes critical operations and data, reflects current conditions, and is approved by senior program managers.
 - Lists resources such as hardware, software, system documentation, and other computer supplies, which support critical operations.
 - Lists facilities housing critical resources.
- 1.3 Develop policies and procedures to:
 - Ensure plans for backup and restoration of all critical applications are complete, reflect changes as they occur, and are checked for accuracy at least semi-annually.
 - Require storing the proper system and application documentation at the off-site location, which are needed for successful recovery of application resources.
 - Require deficiencies disclosed during disaster recovery testing be corrected, and verified when possible, prior to the next disaster recovery exercise.
 - Require applications testing be performed by day-to-day users of the system during disaster recovery testing to ensure all needed data and screens are available. At a minimum, day-to-day users should review the documented results of the applications testing.

Department of Social Services Comments

The Director of the Department of Social Services documented his comments in a letter dated April 29, 2003, which is reprinted in Appendix II, page 25.

2. Adequate Controls Have Not Been Established to Safeguard Access to Sensitive Information

The department is at risk of having current and former employees gain unauthorized access to DCSE's computerized system and sensitive information. Improvements are needed in controlling access to DCSE's computerized system because department personnel have not (1) always followed procedures when revoking employee user IDs, and resetting user's passwords; (2) restricted employees' sharing of user IDs and passwords, or employees' use of multiple user IDs; (3) always conducted criminal background checks on employees; (4) reviewed access rights of users, and controlled access to security software; and (5) restricted access to the system by users from remote locations.

Department procedures for revoking user IDs were not always followed or timely

Department personnel, as well as non-department users, have not always followed procedures to revoke user IDs in a timely manner for all eligible employees. Instead of sending the proper paperwork to the technical support division to revoke a user ID on the day of termination, system users have relied on department technical support division personnel to revoke user IDs based on technical support division monthly reports. When a department employee, or a non-department user, terminates or no longer needs access to DCSE's computerized system, the user's supervisor is required to send completed paperwork to the technical support division to revoke the employee's user ID.

The technical support division also produces a monthly report matching department system users against terminated department employees to find terminated employees' user IDs still active in the system. User IDs on this monthly report are automatically revoked. Technical support division personnel can also revoke user IDs for non-use off their "inactivity" report. The monthly inactivity report identifies department employees who have not used their user IDs to access mainframe applications in six months and non-department personnel who have not used their IDs in three months.

We reviewed a statistical sample of 98 user IDs⁶ revoked during fiscal year 2002 and found 19 user IDs, or 19 percent of our statistical sample of 98 user IDs, were revoked because these individuals had not used department systems housed on the data center's mainframe for specified time periods. Based on our analysis, we estimate the number revoked due to inactivity ranged from 226 to 460 based on a 90 percent confidence level and a study population of 1,708 user IDs.

We also found supervisors did not prepare paperwork to revoke 52 user IDs, or 53 percent, of terminated/transferred employees/non-department users. Based on our analysis, we estimate the number of revoked user IDs in which the user's supervisors did not prepare paperwork ranges from 760 to 1,050 user IDs, based on a 90 percent confidence level and a study population of 1,708 user IDs revoked during fiscal year 2002.⁷

⁶Personnel using these IDs had access to DCSE's data on the computerized system.

⁷See Appendix I, page 23 for additional information.

We also found the following problems related to relying on the technical support division's monthly reports of terminated employees, and/or inactivity, to revoke user IDs.

- State employees have been mistakenly entered as contracted workers on the department's system and would not show up on the monthly report of terminated employees. According to security personnel, these employees should eventually be identified and IDs revoked through the monthly inactivity report. However, this method is only effective when other employees have not used the terminated employees' IDs and passwords.
- Terminated employees transferring directly to another agency were not always shown as terminated employees on the state's computerized payroll system and would not be included on the technical support division's monthly reports.

Revocation of user ID access has not been timely

Our review of sampled user IDs revoked during fiscal year 2002 showed it took an average of 35 days to revoke access rights from the day of termination, transfer, or end of contracted job. According to the FISCAM, termination and transfer procedures should require the division to notify security managers of terminations. Prompt termination of access to the entity's resources and facilities (including passwords) is important. Also, terminated employees who continue to have access to critical or sensitive resources pose a major threat to the organization, according to the FISCAM. Additionally, the FISCAM states an organization could be at risk of failing to detect continual unauthorized actions, if it does not revoke access for employees who no longer need this access.

Procedures for revoking user IDs do not address division systems

Department guidance does not address terminating user IDs when employees have not accessed DCSE's computerized system for three- or six-month time periods. Users access all department systems housed on the data center's mainframe using the same user ID and password. The department's procedures for revoking IDs based on the three- or six-month inactivity periods uses the last date the user accessed any of the department's systems housed on the mainframe. Therefore, a user may not have accessed DCSE's system; however, because the user had accessed another department system housed on the mainframe, the user would be considered an active user and not show up on an inactivity report. According to the FISCAM, inactive user accounts on a computerized system should be monitored and removed when not needed.

According to security personnel, the department does not address division systems because the user's supervisor should forward the proper paperwork to the technical support division when a department employee no longer needs access to one of the computerized systems. In addition, technical support division personnel developed the inactivity report for the department as a whole, not for individual computerized systems, according to security personnel. However, as stated above, many users' supervisors are relying on the department's monthly termination and inactivity reports to ensure user IDs are properly revoked.

User passwords have not been reset in accordance with procedures

Department personnel have not always followed procedures for resetting users' passwords. A password has to be reset when an incorrect password has been entered too many times and the user has been locked out of the system. The password also has to be reset when a user has forgotten his password. Department guidance requires system users to provide identification information before department personnel reset their passwords.

To test department procedures, we contacted department personnel to have a password reset. However, department personnel did not ask for identification information. Instead, they told us the password had been reset to specific identifying information only the user would know. In addition, even though department personnel do not verify the identify of the caller, the caller must know the identification information of the user in order to access the user ID with the reset password, according to department personnel. To test these procedures, we again contacted department personnel and requested them to reset a different password and department personnel divulged the specific identifying information included in the password without verifying the caller was the user in question. We informed the security official of this problem and he took corrective action by directing department personnel to follow established procedures when resetting users' passwords.

Employees share IDs and passwords and use multiple IDs

User IDs and passwords of former employees have been shared after the employee has been terminated. For example, during another State Auditor's Office review, DCSE personnel provided auditors with a terminated employee's user ID and password, without resetting it, to access the computerized system. Using the ID, auditors found they had "add" and "update" access rights in addition to the expected "inquiry" access.

The terminated employee's user ID had been used at 15 terminals after the employee's department termination date. The employee had used the ID on two terminals on the employee's new job at the Department of Health and Senior Services, but had not accessed DCSE's computerized system screens. Auditors, on the review discussed above, used four other terminals. In addition, personnel at two department locations used nine terminals to access DCSE's system screens.

Our review of procedures at a selected field office also disclosed new DCSE technicians are allowed to use their supervisors' user IDs until their IDs have been issued. Department policy states personal identifications and passwords for mainframe programs, such as child abuse records and client case records, should not be shared with anyone under any circumstances.

We found 15 division employees had been issued multiple IDs, and 2 of the 15 employees were located in field offices and had been issued two or more user IDs. Technicians are assigned case files based on geographical locations and can only make changes to a case located in their "primary office," according to a DCSE official. In addition, each user ID can only have one primary office. If a caseworker is assigned cases from two or more offices, the caseworker must be flagged as "primary" in each office. Since a user ID can only be primary in one office, the

user will be issued two, or more, user IDs. Good business practices dictate security personnel only issue one user ID to each user.

Personnel circumvent security measures by using multiple user IDs

DCSE, through the contractor who developed the computerized system, established security procedures—referred to as the Security Matrix—to restrict access rights to some information when the user has access to certain other information.⁸ However, division personnel circumvent this procedure by setting up additional user IDs for individuals so they can have access to restricted information. For example, 13 of the 15 division employees had been issued additional user IDs which resulted in bypassing established security controls. Further review disclosed 7 of the 15 employees had access to DCSE's special functions section intercept group and DCSE's locate group. Users in the special functions section intercept group, normally cannot access the locate group, and vice versa. The intercept group can authorize refunds and release disbursements; whereas, the locate group cannot. The locate group can access and change personal case information, such as financial asset, real estate, and vehicle asset information, but the intercept group cannot. By giving an employee two user IDs to access both groups, DCSE personnel bypassed established access controls.

Guidance provided by the National Institute of Standards and Technology states (1) logical access controls provide a computerized way of regulating what information users can utilize, the programs they can run, and the changes they can make; and (2) the principles of segregation of duties and least privilege are two general principles applied when programming access controls. DCSE's security software has been programmed to restrict users' access to the division's computerized system through pre-defined groups of access rights. Each group has its own level of access or access rights. Some groups have the ability to only read data, whereas other groups can read, add, and delete information from the system.

In commenting on a draft of this report, a DCSE official stated additional user IDs were issued temporarily to employees on special assignments. The 13 employees cited above were issued additional user IDs for that purpose, according to the official. However, even though the additional user IDs were issued temporarily, this practice circumvented security matrix rules.

Criminal background checks have not always been conducted

Department personnel did not check backgrounds on 12 newly hired department employees, or 13 percent of a statistical sample of 93 newly hired, or newly transferred, employees with access to DCSE's computerized system. Based on our analysis, we estimate the number of newly hired department employees with no background check ranges from 66 to 168 employees, based on a 90 percent confidence level and a study population of 850 newly hired or newly transferred employees from fiscal year 2002. The department's Division of Family Services (family

⁸ Access is the ability to take an action, read, add, update, or delete, on DCSE's computerized system. Access control is the method with which DCSE controls users' abilities on the system.

services) and DCSE personnel officers stated they did not know why the background checks had not been completed for the 12 individuals in question.

We also found four newly transferred department employees had not had background checks performed for their most recent positions. Based on our analysis, we estimate the number of these employees having access to DCSE's computerized system ranged from 13 to 79 employees, based on a 90 percent confidence level and a study population of 850 newly hired, or newly transferred, department employees.

According to department human resources personnel, background checks are to be performed after employees begin working for the department. DCSE and family services policies require background checks on all newly hired employees or employees taking new positions in a different DCSE or family services office, according to DCSE and family services personnel officers. New employees should complete the background check forms included in new employee packets, then the division's personnel office forwards the forms to the department's Division of Legal Services, which conducts the checks, according to a human resources officer.

According to National Institute of Standards and Technology guidance, an organization should describe the conditions under which not checking a new employee's background is allowed and any compensating controls to mitigate any risk. However, there are no compensating controls to mitigate this type of risk, according to a DCSE official.

DCSE lacks policies on reviewing user access rights

As of December 31, 2002, DCSE had not established formal policies requiring reviews of user access rights for users of DCSE's computerized system. According to DCSE personnel, DCSE has recently started reviewing levels of access for the system. However, these reviews were based on job titles and focused on the level of access each job title needs, not on determining who does (or does not) need access to the system. According to the FISCAM, access to sensitive information should be limited to only those individuals who actually need access to perform their duties, and system owners should periodically review access authorization listings and determine whether they remain appropriate. Because DCSE is the system owner, DCSE would be responsible for reviewing the appropriateness of user access.

Unrestricted access to sensitive information has resulted in abuses

DCSE policies allow all technicians department-wide access to view sensitive information relating to custodial or non-custodial parents and related child support payments. However, we found technicians, on occasion, have misused their access. DCSE has issued 12 reprimands and suspensions in the past 4 years to DCSE personnel who have inappropriately accessed and/or misused sensitive computerized information. The following are examples of abuses by technicians.

In the first example, a DCSE technician rented an apartment to a custodial parent. When the custodial parent did not pay her rent, the technician looked up the renter's case in DCSE's computerized system to determine whether the custodial parent had received a child support payment. Since she had received it, the technician told the custodial parent she should be able to pay her rent. Officials suspended this technician. In the second example, officials suspended another technician for accessing the system and providing screen prints of information to a friend relating to the friend's case.

Examples of
misuses of
sensitive data

In these examples, DCSE personnel stated the only way to view this information would be to do it at a case level. Therefore, if employees only had access to their assigned cases, they could not access sensitive information related to other child support cases, according to a DCSE official. According to the official, when a technician is party to a case handled at the technician's field office, the case must be moved to a different field office. All technicians can view cases; however, only DCSE technicians working in the office where the case is handled can access the case to make changes to case related information. Such changes would include changing payment information or information related to court actions.

In the third example, officials reprimanded a technician for accessing the computerized system to obtain the phone number of the custodial parent's employer on a friend's case. She then called the employer and attempted to obtain information on health insurance.

In this example, the employee did not have to access the friend's case to obtain the information. However, technicians have department-wide access to view and change "member" information such as an individual's address on a case. Therefore, the employee could view information on the non-custodial parent of her friend's child without accessing case sensitive information. Restricting access to member information has been reviewed by DCSE personnel. However, they have not found a "viable automated solution" to this problem, and the division did not maintain documentation supporting the review, according to a DCSE official.

Improvements are needed in handling security violations and suspected incidents

DCSE personnel officers log all personnel reprimands, including reprimands for inappropriate computer system accesses. However, the personnel officers have only maintained a log of proven incidents on DCSE's computerized system resulting in reprimands, not suspected incidents. In addition, reprimands have not been reported to senior division management because personnel actions are considered confidential and the division's personnel officer said most reprimands are not security violations. Instead, they represent inappropriate use of the employee's authorized access, according to a DCSE personnel officer. Once senior management hands the case over to personnel officers, officials do not follow up on the suspected incidents. Technical support division personnel are only involved if they are asked to generate activity reports for personnel officers for the investigation and do not follow-up on suspected incidents.

According to a DCSE personnel officer, DCSE's personnel unit does not maintain logs of suspected incidents because, in most cases, by the time this unit is notified of these incidents, the employees have already been recommended for disciplinary action. Most unsubstantiated cases are not reported to division personnel, according to a DCSE personnel officer. Also, according to a DCSE official, division management does not follow-up because personnel issues are sensitive and the official does not believe division management needs to know about the reprimands. However, the FISCAM states, if a security violation has occurred, the control weakness allowing the breach to occur should be corrected. The FISCAM also states it is important an organization have formal written procedures for reporting suspected security violations to security management so trends can be identified, system owners can be alerted to potential threats, and appropriate investigations can be performed.

Tracking access has not been adequate

The department's security manual has not been updated regarding audit trails reviewed by the department's technical support division personnel. According to the code of federal regulations,⁹ DCSE personnel should monitor access to, and use of, the computerized child support enforcement system through audit trails and a feedback system to identify and prevent unauthorized access or use. The FISCAM defines an audit trail as a step-by-step history of a sensitive transaction. An audit trail can include source documents, electronic logs, and reports of accesses to restricted data.

As of July 2002, there were three audit trails listed in the department's security manual that were to be reviewed, and at that time, those audit trails were not being reviewed. However, during the course of our audit, the security group began reviewing a total of six audit trail reports. As of December 2002, security group personnel were still trying to determine the exact format of the audit trail reports and the proper follow-up procedures to apparent access violations.

Access to security software has not been properly restricted

The department has not established formal policies and procedures requiring the technical support division's security officer to review employees with group special access to security software, and prior to our audit, no reviews had been performed. The FISCAM states access to the security software should be restricted to a limited number of authorized persons within the security function to minimize the risk of unauthorized changes.

As of December 31, 2002, there were 14 technical support division users and one Department of Health and Senior Services user authorized to make changes through security software. The security software is used by the data center and the technical support division to restrict access to computer systems. Six of the 14 technical support division users with access to the security software are in the security group and should have the ability to add users to the system and administer access rights. However, after our inquiry on January 7, 2003, security group

⁹45 CFR 307.13.

personnel determined three users no longer needed this special access. In addition, the Department of Health and Senior Services employee will have special authority revoked because security group personnel determined it is no longer appropriate. However, these users were not actually revoked until we made a follow-up call on February 6, 2003 to determine if the revocation had been completed.

Five of the 14 users were not in the security group and, as of January 31, 2003, had not been reviewed by the security officer to determine whether they needed special access to security software. According to technical support division personnel, prior to 1992, these employees were in the group responsible for the functions the security group is now administering; therefore, these employees needed the ability to make changes through the security software. Even though the security group has taken over those responsibilities, these five employees retained the ability to make changes through security software. Technical support division personnel stated reviewing the access rights of these five employees is something either the security official or their group manager will have to do. Personnel also stated there is no set time or assurance it will be done. The FISCAM states access to very sensitive resources, such as security software programs, should be limited to very few individuals and users should only have the access needed to perform their duties. Additionally, the FISCAM states access rights should be periodically reviewed to ensure they remain appropriate.

Dial-up access to the computerized system has not been properly restricted or reviewed

The department's policies and procedures address granting general access to the department's computerized systems. However, policies and procedures do not specifically address granting access from a remote location using a modem. Additionally, users with dial-up access are not periodically reviewed to ensure access is appropriate. The FISCAM states access to the computerized system through dial-up should be limited because dial-up access can considerably increase the risk of unauthorized access, and system owners should periodically review access authorization listings.

DCSE's security officer provided us with a listing of 48 division computerized system users with dial-up access, which we determined to be inaccurate. We requested the same information from the data center's contractor who owns the dial-up software. The contractor's listing showed a total of 345 dial-up users with access to the system, and the last date each individual used the dial-up software. We noted that 263, or 76 percent, of the 345 dial-up users did not use dial-up capabilities during calendar year 2002. We also found one individual who transferred to the Department of Health and Senior Services in June 2002, who had dial-up access to DCSE's system until January 2003. At that time, due to our inquiries, technical support division personnel reviewed the listing of dial-up users and determined the individual no longer needed access to the system.

DCSE's security officer knew many users have dial-up access to DCSE's computerized system. However, the security officer indicated most of these users were not DCSE employees, and therefore, had read-only access to the system. She also stated security officers in each division have responsibility for their own employees' dial-up access. Prior to our initial inquiry, DCSE had not reviewed authorization listings to determine whether dial-up users still need access to its

system. As of February 25, 2003, DCSE is working with technical support division personnel to determine whether all division employees having access actually need access. Those users no longer needing dial-up access will lose this access, according to the DCSE security officer. Additionally, the security officer stated DCSE plans to periodically obtain a contractor generated listing of users with dial-up access from the technical support division and review it to ensure all users with the access still need this access. However, as of February 25, 2003, DCSE has not created formal policies and procedures for this review.

Conclusions

Department personnel, as well as non-department users, have not always followed procedures for revoking employee user IDs, and instead have relied on the department's technical support division personnel to revoke user IDs. Revocation of user IDs has not been timely and procedures for revoking user IDs have not addressed revoking user IDs when personnel have not accessed DCSE's computerized system for specified time periods. Because DCSE owns the data, it is DCSE's responsibility to ensure user IDs are revoked promptly. Department personnel also have not always followed procedures for resetting users' passwords. User IDs and passwords of former employees have also been shared after the employee has been terminated, and new DCSE employees are allowed to use supervisors' IDs. Personnel have issued multiple user IDs, in some cases circumventing security measures. By not following procedures for revoking employee IDs, resetting users' passwords, and allowing the sharing of passwords, department employees incur unnecessary risk unauthorized personnel can access sensitive information in DCSE's computerized system.

Criminal background checks have not always been conducted on newly hired or newly transferred employees, with access to DCSE's computerized system. DCSE personnel also have not established controls to mitigate the risk associated with individuals having access prior to completion of background checks. Not conducting background checks on employees, or establishing risk mitigation controls, also increases the risk of personnel accessing and misusing sensitive DCSE data.

DCSE had not established policies and procedures requiring reviews of user access rights. Additionally, technicians have access to all cases, not just those cases in their respective caseloads. Unrestricted access to sensitive information has led to some abuses at DCSE. Access violations, or suspected violations, on the division's computerized system are not tracked and reported to DCSE management. Policies and procedures for reviewing audit trails are not accurate and up-to-date. The department also has not properly restricted access to security software, and prior to our audit, no reviews had been performed in this area. Access to very sensitive resources, such as security software programs, should be limited to very few individuals. The department does not have policies and procedures to ascertain whether users still need this access. The department also does not have policies and procedures for granting access to DCSE's system via dial-up, or determining whether users still need remote dial-up access. Until these issues are resolved, DCSE cannot be assured sensitive computerized information is protected against unauthorized access and misuse.

Recommendations

We recommend the Director of the Department of Social Services require:

2.1 DCSE officials to:

- Ensure paperwork is completed and remitted timely to the technical support division when revoking user IDs for employees and non-department users who terminate, transfer, or no longer need access to DCSE's computerized system.
- Ensure employees do not share user IDs and passwords, and employees are not allowed to use multiple user IDs.
- Discontinue issuing multiple user IDs that result in bypassing security protocols.
- Track all suspected DCSE system access violations and report all suspected and proven violations to division management.
- Document policies and procedures for periodically reviewing user access rights for DCSE system users.
- Review policies allowing technicians read-only access to all cases and update access to all members on DCSE cases, to determine if this access is actually needed for the technicians to perform their duties.
- Develop specific policies and procedures for granting dial-up access to the computerized system. Additionally, this access should be reviewed periodically to ensure it remains appropriate.

2.2 The department's technical support division to:

- Establish a process for monitoring inactive user IDs, specifically for DCSE's computerized system.
- Ensure department password resetting protocols are properly followed.
- Develop accurate and up-to-date policies and procedures for reviewing audit trails, including who is responsible for reviewing audit trail reports and what follow-up action should be taken on apparent access violations.
- Develop policies and procedures to ensure only appropriate employees have access to make changes through security software.

2.3 Department officials to:

- Ensure criminal background checks are properly performed and documented on each newly hired or newly transferred employee with access to DCSE's computerized system.

Department of Social Services Comments

The Director of the Department of Social Services documented his comments in a letter dated April 29, 2003, which is reprinted in Appendix II, page 25.

SAMPLE METHODOLOGY AND RESULTS

This appendix describes how we identified study populations and our sampling methodologies for two statistical samples.

Audit Universe for Revoked Users IDs

To measure the number of user IDs revoked due to the monthly reports of terminations and inactivity, we reviewed a statistical sample of 98 user IDs from a study population of 1,708 user IDs, provided by DCSE, revoked during state fiscal year 2002. We based sample size on a 90 percent confidence level with a 7 percent precision and an expected error rate of 25 percent.

Based on the results of the sample, we estimate 53 percent of the study population, or 906 user IDs were revoked based on the monthly report of inactivity after the user's termination, transfer, or end of contracted job. Table I.1 displays sample results.

Table I.1: User IDs Revoked Through Termination Reports

Category	Result
Sample Size	98
IDs revoked without proper paperwork submitted	52
Point estimate error rate	53%
Point estimate quantity	906
Upper limit error rate	62%
Upper limit quantity	1,050
Lower limit error rate	45%
Lower limit quantity	760

We estimate 19 percent of the study population, or 331 user IDs, were revoked due to inactivity, but the users did not terminate, transfer, or end a contracted job. These users were current employees who simply did not use their access for the specified period of time. Table I.2 displays sample results.

Table I.2: Current Employees Revoked Due to Inactivity Reports

Category	Result
Sample Size	98
IDs revoked without proper paperwork submitted	19
Point estimate error rate	19%
Point estimate quantity	331
Upper limit error rate	27%
Upper limit quantity	460
Lower limit error rate	13%
Lower limit quantity	226

Audit Universe for Background Checks

To measure the number of newly hired or new transferred department employees, with access to the DCSE's computerized system, who had not had background checks, we reviewed a statistical sample of 93 user IDs from a study population of 850 newly hired or newly transferred department employees, provided by the department, who have access to DCSE's computerized system. We based sample size on a 90 percent confidence level with a 7 percent precision and an expected error rate of 25 percent. We also measured the average number of days it took to perform a background check from the date of hire or transfer to new position.

Based on the results of the sample, we estimate 13 percent of the study population, or 110 department employees, had not had any background checks performed on them since they started employment with the department. Table I.3 displays sample results.

Table I.3: Users With No Background Checks Performed

Category	Result
Sample Size	93
Department users hired with no background checks performed	12
Point estimate error rate	13%
Point estimate quantity	110
Upper limit error rate	20%
Upper limit quantity	168
Lower limit error rate	8%
Lower limit quantity	66

We estimate 4 percent of the study population, or 37 employees, had not had any background checks performed on them in their most current positions within the department. Table I.4 displays sample results.

Table I.4: No Background Check Performed for Current Position

Category	Result
Sample Size	93
Department users transferred to positions with no additional background checks performed	4
Point estimate error rate	4%
Point estimate quantity	37
Upper limit error rate	9%
Upper limit quantity	79
Lower limit error rate	2%
Lower limit quantity	13

COMMENTS FROM THE DEPARTMENT OF SOCIAL SERVICES



MISSOURI
DEPARTMENT OF SOCIAL SERVICES
P. O. BOX 1527
BROADWAY STATE OFFICE BUILDING
JEFFERSON CITY
65102-1527
TELEPHONE: 573-751-4815, FAX: 573-751-3203

BOB HOLDEN
GOVERNOR

Steve Rolling
DIRECTOR

RELAY MISSOURI
for hearing and speech impaired
TEXT TELEPHONE
1-800-735-2966
VOICE
1-800-735-2486

April 29, 2003

Honorable Claire McCaskill
Missouri State Auditor
P.O. Box 869
Jefferson City, Missouri 65102

Dear Ms. McCaskill

Below is the response of the Department of Social Services to your audit of the
"Division of Child Support Enforcement Computer Risk Management Program."

Risk and Disaster Plans

The Department of Social Services has a disaster recovery plan that covers all the major computer systems in the Department. The Missouri Automated Child Support System used by Division of Child Support Enforcement is just one of those systems.

Risk and disaster planning along with security controls in the computer operations of the Department of Social Services (DSS) and its Division of Child Support Enforcement (DCSE) have dramatically changed and improved during the period covered in this audit. From inception in 1994 until September of 2001 the main DCSE computer system (Missouri Automated Child Support System - MACSS) was under the complete control of a private contractor. During that period the development firm was fully responsible for risk assessment and disaster recovery. Since September of 2001, the Information Services and Technology Division (ISTD) has become responsible for this computer program and its operation and maintenance. Also during the audit period, the control and maintenance of the Department's mainframe computer hardware was shifted from the Department to the centralized State Data Center in 1997. Since then, risk management, data storage and disaster recovery of these 'hardware' items are under the control of the centralized State Data Center.

Moving the control of the MACSS system from a private contractor to the Department's Information Technology shop and consolidating computer hardware at the centralized State Data Center have provided substantial savings to the taxpayer. Fully implementing risk management programs, disaster recovery planning and security activities are an ongoing process of the Department and the State Data Center.

The 2003 disaster recovery test referenced in the audit, proved that by following the existing disaster recovery plan the Department can successfully bring all 47 computer program areas into operational condition within 3 days of a mock "major debilitating state disaster." Since the disaster recovery test in 2001, DSS has made continual improvement to the point where the DCSE system (along with many others) was up and operating within 72 hours.

"AN EQUAL OPPORTUNITY/AFFIRMATIVE ACTION EMPLOYER"
services provided on a nondiscriminatory basis

Honorable Claire McCaskill

Page 2

From the successful 2003 disaster recovery test the Department can now prepare the additional documentation suggested by the auditor. DSS agrees with the audit recommendation and had already started work on a comprehensive risk management program by obtaining information protection assessment software from the Computer Security Institute and establishing a cross functional team within ISTD to oversee this project. DSS will adopt a policy to ensure disaster recovery policies and procedures are reviewed on a regular basis.

Security Controls

There are numerous components to an effective system of computer security controls. DSS has a fully developed system of electronic user IDs and passwords integrated into a Department wide security approval system for tracking those who have access to the DSS computers. This is a department wide system that includes the Child Support system.

In addition to the various department wide controls on access to the computer system, a security matrix exists within the MACSS computer system that restricts access to data depending on the employees user ID. Under the security matrix and user ID system, only those employees whose positions use and need access to sensitive information are given access. It is this added level of control and restriction that has given rise to the limited need for some employees to be given two user IDs.

Because of the restriction associated with each ID, the system will not allow an employee to have multiple location assignments or the access to perform duties outside their job assignment. To accommodate these situations and still maintain security, the employee who needs additional access is assigned separate IDs for each situation. This allows DSS to maintain all existing controls and track the actions of these employees in each special situation.

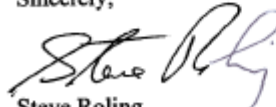
When an employee misuses the access provided their position through the ID and security matrix system in DCSE, personnel actions have and will follow. An employee's misuse of properly authorized access is a personnel issue. The Department has always investigated these situations and taken strong action when misuse is found.

"Dial up access" permits employees to access the system from a remote location and do their work while on the road or at an alternate work location. Existing security protocols require the employee to have a valid security clearance associated with their valid user ID, otherwise "dial up" gets no access to information. DSS will periodically review the users continued need for the dial up.

DSS will consider centralization of the new-hire background checks to improve timeliness and documentation. DSS will work with managers and supervisors to improve compliance with existing policies that the security access of terminated or transferred employees be revoked in a timely manner. Each of these actions will help ensure full compliance with existing Department policy.

I appreciate the opportunity to respond to the findings in this audit.

Sincerely,



Steve Roling
Director

SR/RS/km